United States District Court
District of New Jersey

UNITED STATES OF AMERICA	:	**COMPLAINT**
	:	
v.	:	**Mag. No. 05-8047 (MCA)**
	:	
JASON SALAH ARABO,	:	
a/k/a "CLdotcom,"	:	
a/k/a "Jaytheplaya"	:	

I, Adam Ringhof, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A
continued on the attached sheets and made a part hereof.

I further state that I am a Special Agent for the Federal Bureau of Investigation and that this complaint is based on the following facts:

SEE ATTACHMENT B
continued on the attached sheets and made a part hereof.

Adam Ringhof
Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,
March 11, 2005 at Newark, New Jersey

HONORABLE MADELINE COX ARLEO
UNITED STATES MAGISTRATE JUDGE

Signature of Judicial Officer

ATTACHMENT A

From on or about July 2, 2004, continuing to at least December 12, 2004, in Edison, Union County, in the District of New Jersey and elsewhere, defendant

JASON SALAH ARABO,
a/k/a "CLdotcom,"
a/k/a "Jaytheplaya,"

did knowingly and intentionally conspire and agree with others to cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer, namely, a computer that was used in interstate and foreign commerce and communication, contrary to Title 18, United States Code, Section 1030 (a)(5)(A)(i).

OVERT ACTS

In furtherance of the conspiracy, defendant ARABO and his co-conspirators committed and caused to be committed the following overt acts, among others, in the District of New Jersey and elsewhere:

1. On or before July 2, 2004, defendant ARABO, via an online communication, recruited another individual to conduct distributed denial of service ("DDOS") attacks on a computer that supported the website of a New Jersey company, in exchange for items of value.

2. On or about November 17, 2004, defendant ARABO mailed to another individual a pair of shoes in payment for DDOS attacks that the individual had conducted.

3. On or about November 20, 2004, defendant ARABO caused another individual to conduct a DDOS attack on a computer that supported the website of a New Jersey company.

4. On or about December 9, 2004, defendant ARABO, via an online communication, offered another individual items of value to conduct a DDOS attack on a computer.

5. On or about December 12, 2004, defendant ARABO, via an online communication, recruited another individual to conduct DDOS attacks on computers that supported the websites of ARABO's competitors, including a New Jersey company, in exchange for items of value.

All in violation of Title 18, United States Code, Section 371.

ATTACHMENT B

I, Adam Ringhof, a Special Agent of the Federal Bureau of Investigation ("FBI"), having conducted an investigation and discussed this matter with other law enforcement officers who have participated in the investigation, have knowledge of the facts set forth below. Because this Affidavit is submitted for the sole purpose of establishing probable cause to support the issuance of a criminal Complaint, I have not included each and every fact known by the United States concerning this investigation. Statements attributed to individuals are provided in substance and in part.

Summary of Relevant Computer and Internet Concepts

1. **The Internet** is a collection of computers and computer networks (including personal computers and computer servers) that are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently crosses state and international borders even where the two computers are located in the same state.

2. **Internet Protocol Address** ("IP address"): An IP address is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots (*e.g.*, 149.101.10.40). Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination.

3. **Internet Service Providers** ("ISPs"): Most individuals and businesses obtain access to the Internet through ISPs. AOL, Microsoft ("MSN"), and Comcast are examples of some of

the larger and better-known ISPs. Other ISPs include private entities such as corporations, universities, and government agencies. ISPs own blocks of IP addresses, which they assign to their customers' computers and networks, enabling customers to access the Internet using telephone, cable, Digital Subscriber Line ("DSL"), or other types of telecommunications lines.

4. **Web Hosting Company**: Web hosting companies install their customers' websites on computer servers, operated and maintained by the hosting company, that are linked to the Internet. Hosting companies can also provide their customers with data storage and communications services such as email and "instant messaging," also via computer servers. A large customer's web-based business may be supported by multiple dedicated computer servers, whereas one server may support a number of smaller customers' websites.

5. **Internet Relay Chat (IRC)** - an IRC is a network of computers connected through the Internet that allows computer users to communicate (or chat) with others in real time. An IRC server is administered by a particular computer user or users (the "operator") who are authorized to control the functions of the IRC. Operators (but not other users) can use IRC servers to control "bots" as described below.

6. **Bot** - The term "bot" is derived from the word "robot" and commonly refers to a software program that performs repetitive functions, such as indexing information on the Internet. Bots can perform tasks automatically, or receive commands from operators via IRC. Although bots have legitimate functions on the Internet (for example, monitoring a user's search requests for new car information, and automatically presenting the user with auto manufacturers' advertisements), bots can be used for malicious and criminal purposes, for example, to flood a corporation's website with repetitive information requests in order to overload and crash the

corporation's computer servers.

7. **Botnet** - a "Botnet" is a network of bots that is commonly employed by malicious operators to control or attack computer systems. Botnets are created by gaining unauthorized access to computers on the Internet and infecting those computers with a particular bot program. The botnet is then controlled by an operator, often through IRC. Operators sometimes post bots on internet websites disguised as MP3 music files or photographs, which unsuspecting computer users then download to their computers, infecting them. Operators also insert bots into vulnerable computer systems by means similar to a computer virus or worm which propagates throughout the Internet. The unsuspecting infected or compromised computers are often referred to as "zombies" or "drones" and are used in distributed denial of service attacks.

8. **DDOS** - a "Distributed Denial of Service Attack" (or "DDOS attack") is a type of malicious computer activity by which an attacker causes a network of computers – for example, the aforementioned "zombie" or "drone" computers -- to "flood" a victim computer with large amounts of data or specific commands. As a result, the victim computer is unable to handle legitimate network traffic and legitimate users are denied the services of the computer. Depending on the type and strength of the DDOS attack, the victim computer and its network may become completely disabled and unable to perform its intended function without significant repair. DDOS attacks also disrupt computers and networks in the Internet that are linked to the victim computer, causing harm such as server crashes and data overloads that hinder or tie up communications.

9. **Synflood** - A particular type of DDOS attack whereby the attacking computer initiates contact with the target computer (typically a server) by sending a "synchronous" or "syn" packet.

The target computer acknowledges that the attacking computer wants to communicate with a "synchronous-acknowledgment" or "syn-ack" packet and then awaits further instructions. This process is part of the normal exchange of data between computers. A synflood occurs when one or more attacking computers send the "syn" to initiate communication, but do not send any additional data. The targeted server will wait for some specified period of time before disconnecting; however, when that lag time is combined with a flood of "syn" packets from attacking computers, it overwhelms the server's ability to respond to legitimate requests.

10. By their nature, and because the Internet is essentially a single network of interconnected computers, synfloods typically cause severe harm and disruption far beyond their targets. A synflood can target a computer server that hosts an online business's website, essentially shutting down the website, and in effect, shutting down the business. Because the targeted server, maintained and operated by an ISP, is linked to other computers in the Internet as described above, the synflood disrupts other websites and services of the ISP's customers, causing collateral harm.

The Investigation

DDOS Attacks on Sports Apparel Online Retailers

11. As described more fully herein, investigators have obtained evidence, including information from a confidential source ("CS") which has been corroborated and/or otherwise proven reliable, which revealed that defendant JASON SALAH ARABO, a/k/a "CLdotcom," a/k/a "Jaytheplaya," ("ARABO"), who at all times relevant to this Complaint owned and operated an online business that sold (among other things) "retro" or "throwback" sports apparel, used a computer located at his residence in Michigan to instigate and direct DDOS attacks

against his competitors, including a company in New Jersey, in violation of federal law.

12. On or about July 7, 2004, the Newark, New Jersey office of the FBI received a complaint from the owner of a New Jersey company with the initials JJ, which was in the business of retail sales of "retro" or "throwback" sports apparel. At all times relevant to this Complaint, JJ was engaged in internet or "e-commerce" via its internet website. The owner of JJ explained to investigators that JJ had experienced a DDOS attack that had effectively shut down its website, which the company used to conduct virtually all of its business. JJ's website was hosted by a third party web hosting company, that is, rather than owning and operating its own computer servers, JJ contracted with the web hosting company, which provided website computer server space to numerous different companies and users. The majority of JJ's revenue was generated via its e-commerce website. JJ's website, via its web hosting company, used one or more computers which operated in interstate and foreign commerce and communication.

13. From on or about July 2, 2004, to on or about December 6, 2004, JJ was periodically under attack by synfloods, which caused the resources of the server handling JJ's website to be tied up and overloaded with syn requests, and therefore rendered the JJ website unavailable to its legitimate Internet customers. Whenever these attacks occurred, JJ was unable to conduct normal business via its e-commerce site. As a result, JJ's volume of business declined dramatically, causing significant financial losses.

14. These DDOS attacks were so severe that they affected service to other customers of the web hosting company which were unrelated to JJ. The web hosting company also lost business from customers who were affected by the disruption to the servers caused by the DDOS attacks and elected to transfer their business to other web hosting companies. As a result, the

web hosting company refused to continue to provide services to JJ.

15. JJ subsequently contracted with at least two other web hosting companies, and each time, synfloods attacked the companies' servers, and the companies similarly refused to provide services to JJ. These two web hosting companies also suffered financial losses from other customers leaving because of the attacks.

16. During the course of the investigation into the DDOS attacks against JJ, investigators learned that, at about the same time as the synflood attacks on JJ, similar attacks were being directed at several other companies which were also in the same type of sports apparel business and sold the same manufacturers' products as JJ. One of these companies was based in Georgia and had the initials DR. Like JJ, DR suffered severe and repeated synflood attacks, which caused disruptions in its e-commerce website and a concomitant loss of business revenue.

17. These repeated synflood DDOS attacks on JJ, DR, and other online retailers also caused significant disruption and harm to other, unrelated online businesses as well as to the ISPs and web hosting companies who supported their online operations. For example, the attacks caused significant harm to a large ISP, based in eastern Pennsylvania, that supported one of JJ's web hosting companies. Dozens of companies supported by this ISP – including at least two based in Europe – lost services such as Internet access, corporate websites, email, data storage and disaster-recovery systems during the attacks. The affected companies included major online retail businesses, banks, and providers of information, communication and data backup for the medical and pharmaceutical industries.

Investigators Trace the Source of the Attacks to a Particular Individual

18. Cyber crime investigators have various methods for tracing the origin of DDOS

attacks. In this case, investigators identified certain "zombie" or "drone" computers which had been infected by a "bot" that investigators identified as having been used in the DDOS attacks on DR and JJ. Student computers on college campuses in Massachusetts and Pennsylvania were among those infected, unbeknownst to their users. Investigators were then able to isolate the "bot" on a test computer and determine what computer was controlling the "bot" by noting what domains/IP addresses the "bot" was attempting to communicate with, and tracing those communications back to the originating computer/IP address.

19. Using this technique, investigators noted that each domain the isolated "bot" attempted to communicate with included the name "Pherk" in the domain name. Investigators thus learned that the originating IP address corresponded to a computer located at a residence in New Jersey, and that the user of this computer and IP address employed the online usernames "Pherk" and "Jatt." Investigators discovered that an individual with the initials "JS" was the person associated with those usernames, and that JS lived at that New Jersey residence. Investigators also discovered a personal website for "Jatt" that listed personal attributes, and included a photograph, that corresponded to the person identified as JS.

20. CS independently informed investigators that, in or about June 2004, an individual with the America Online (AOL) Instant Messenger username "CLdotcom" had attempted to recruit CS to conduct computer attacks against certain sportswear-apparel companies – among other things, to hack into their servers and render them inoperable, and to access and steal their customers' email addresses. CS learned that CLdotcom owned an online business known as Customleader.com, which was a competitor of JJ, DR and other online retailers of "retro" sports apparel. At that time, CS told CLdotcom that he could not undertake such attacks, but referred

CLdotcom to an individual known by the online username of "Jatt," and by another online name, "Pherk," and who CS knew to be capable of committing the types of attacks CLdotcom had requested. CS knew that "Jatt" a/k/a "Pherk" commanded a large botnet that was capable of launching a formidable DDOS attack that could accomplish the destructive aims CLdotcom had expressed.

21. Based on the evidence described in the preceding paragraphs, investigators concluded that JS was the individual who conducted the attacks against JJ, DR and others using a computer located at JS's home in New Jersey. On or about December 6, 2004, a federal search warrant was executed at JS's residence. A number of items of evidence were seized including several computers, sports apparel (including athletic shoes) and a watch.

Investigators Discover JASON ARABO, a/k/a "CLdotcom"

22. JS (a juvenile) agreed to answer investigators' questions, and stated that JS had indeed conducted DDOS attacks upon JJ, DR and other companies at the behest of an individual JS had communicated with online via instant messaging who used the online username "CLdotcom." JS also stated that "CLdotcom" had compensated JS for said DDOS attacks in the form of the sports apparel and watch that were seized.

23. JS further stated that CLdotcom had provided lists of companies he wanted "taken down," or otherwise compromised enough so that those companies would be unable to conduct online commerce. These lists included JJ and DR, among others. CLdotcom had praised the success of JS's DDOS attacks, and told JS that his business was better on the days of the attacks.

24. JS confirmed that JS controlled a botnet comprising approximately 2,000 bot-infected computers that JS used to conduct DDOS attacks, and that JS controlled the botnet

through an IRC.

25. Investigators have since determined that CLdotcom was an online name used by defendant ARABO, in connection with the charged offense, as described further herein.

26. On or about December 17, 2004, investigators accessed the **www.customleader.com** website and observed a message stating: "We have moved! We have moved our website and changed our name to Jersey Domain." Investigators observed that visitors to the **www.customleader.com** website were automatically redirected to another website, **www.jerseydomain.com.** Jerseydomain.com advertised itself as an online business that specialized in selling retro and throwback college and professional sports jerseys. These jerseys were the same type as those sold by DR and JJ.

27. The mailing address of **www.jerseydomain.com** appearing on its website was Jersey Domain, P.O. Box 4234, Southfield, Michigan, 48037, and its business phone number was 1-888- Jersey-8. Postal records indicated that the registered renter of P.O. Box 4234 was defendant JASON ARABO, with an address in Southfield, Michigan. Investigators have determined that this address was defendant ARABO's residence, and that he operated **www.jerseydomain.com** out of that residence.

ARABO Recruits Another Individual to Conduct DDOS Attacks

28. On or about December 9, 2004, an undercover investigator ("UC") posing as and using the identity of CS with CS's permission, recorded a series of AOL instant-message "chat" communications between UC and defendant ARABO, who used the online name "CLdotcom" for such communications. In this conversation, ARABO told UC that he had previously recruited Jatt to conduct a series of DDOS attacks against several online companies. In addition,

ARABO told UC that Jatt's DDOS attacks had not done enough to keep the online victim companies down. In this same conversation, ARABO propositioned UC to commit DDOS attacks against online sports apparel merchants. ARABO told UC that he could get sports apparel and watches as payment to conduct these DDOS attacks.

29. On or about December 12, 2004, investigators conducted and recorded two additional online "chat" conversations between UC and defendant ARABO, who again used the online name "CLdotcom." UC informed ARABO that UC had gained "root" access to JJ's server, which would allow insider access to JJ's customer lists, financial information, web access controls and other sensitive data stored on JJ's server. UC offered to send JJ's sensitive data to ARABO via file transfer protocol ("ftp"), which is a means to transfer large volumes of computer data. Defendant ARABO refused UC's offer, stating "they trace IPs," indicating his fear that if an ftp file were transferred to him, law enforcement would be able to trace this unlawful intrusion back to ARABO.

30. During this same online "chat," ARABO asked UC to "take down" JJ's server from within by using UC's "root" access, and to delete its database of customers. ARABO also asked UC to redirect all of JJ's website traffic to a pornographic website so customers attempting to connect to JJ's website could not find it. ARABO repeatedly instructed UC to "hit them hard." ARABO then again offered UC sports apparel, a watch and jewelry as payment to conduct a DDOS attack on JJ, DR and other companies.

31. During a second online "chat" the same day, defendant ARABO, still using the online name "CLdotcom," again propositioned UC to conduct a DDOS attack against several online companies. ARABO listed five specific online companies he wanted UC to attack. The

list of companies again included JJ and DR.

32. On or about December 22, 2004, a search warrant was executed at the residence of defendant ARABO. Agents discovered, among other things, new athletic apparel, including throwback sports jerseys of the type sold by JJ and DR, and athletic shoes and a watch of the types CLdotcom had given to JS as payment for conducting the DDOS attacks.

33. When the search warrant was executed, ARABO agreed to be interviewed by investigators. ARABO stated that, using the online name CLdotcom and communicating via instant messaging, he hired "Jatt," a/k/a JS, to execute DDOS attacks against his competitors' websites, including JJ and DR. He further stated that he had compensated Jatt with, among other things, athletic apparel. Arabo stated to investigators that he selected JJ and DR for attacks because they were the most popular online retailers for "throwback" sports merchandise. Arabo also stated that he believed by shutting down the websites and online operations of JJ and DR, his own business would grow and become as popular as the victim companies.